IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH goldmusicsoul3@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 24-mj-1622 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Francis Nero, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Philadelphia Division, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since May 2011. Prior to joining the FBI, I was an Assistant District Attorney with the Montgomery County District Attorney's Office assigned to Major Crimes. I am a graduate of

the FBI Academy in Quantico, Virginia. I am currently assigned to the FBI Philadelphia's Allentown Resident Agency to investigate Violent Crimes Against Children (VCAC), whose primary mission is to investigate those individuals and groups that are engaged in the criminal sexual exploitation of children. During my tenure as an FBI agent, I have participated in many investigations pertaining to individuals and groups involved in criminal exploitation of children, to include possession and distribution/receipt through electronic means of child sexual abuse material (CSAM) (hereafter "child pornography" as defined by statute), manufacturing child pornography, transportation of a minor to engage in criminal sexual activity, and child sextortion violations. I have personally conducted numerous investigations involving violations of these laws, which have resulted in the arrest of individuals who have committed these violations of the federal criminal code.

3. As a federal agent, I am authorized to investigate violations of laws of the United States and am a "federal law enforcement officer" within the meaning of Fed. R. Crim. P. 41(a)(2)(C).

4. The statements in this affidavit are based on my investigation and other law enforcement officers' investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of certain federal laws, to include violations of 18 U.S.C. § 2252(a), are located at premises owned or maintained by Apple Inc. (Apple) and associated with the iCloud account goldmusicsoul3@gmail.com.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

LEGAL AUTHORITY

6. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, or attempts to do so.

7. "Visual depictions" include data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (*See* Title 18 U.S.C. § 2256(5)).

8. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital to genital, oral to genital, or oral to anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. (*See* Title 18 U.S.C. § 2256(2)).

9. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), cert. denied, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is

sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), aff'd sub nom, *United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), aff'd, 813 F.2d 1231 (9th Cir. 1987), cert. denied, 484 U.S. 856 (1987). The *Dost* factors include: (1) whether the focal point of the visual depiction is on the child's genitalia or pubic area; (2) whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity; (3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child; (4) whether the child is fully or partially clothed, or nude; (5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity; and (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer. *See also United States v. Villard*, 885 F.2d 117, 122 (3d Cir.1989). Significantly, "[a] visual depiction need not involve all of these factors to be 'lascivious exhibition' of the genitals or pubic area." *Dost,* 636 F. Supp. at 832. The determination is based on the overall content of the visual depiction, taking into account the age of the minor. *Id.; see also Villard*, 885 F.2d at 122 ("Although more than one factor must be present in order to establish lasciviousness, all six factors need not be present.").

10. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Apple. I request that Apple be required to produce the electronic communications and other information identified in Attachments A and B hereto. Because Apple is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Apple to perform the search would be a burden upon the company. If all Apple is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Apple to search the materials to determine what content is relevant would add

to its burden.

11. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B from what is produced by Apple pursuant to the search warrant. In reviewing these files, I or other law enforcement agents will treat them in the same way as if we were searching a file cabinet for certain documents. E-mails and chat logs will be scanned quickly to determine if they are relevant to our search. If they are, they will be read. If we determine that they are not relevant, we will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

12. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

13. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Apple to comply even though Apple is not located in this district, because the Court has jurisdiction over the offense being investigated.

14. I also ask that the warrant direct Apple to produce records and other information pertaining to this account. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth below to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

15. This application seeks a warrant to search all responsive records and information under the control of Apple, a provider subject to the jurisdiction of this Court, regardless of where Apple has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Apple's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

BACKGROUND OF THE INVESTIGATION

16. In August 2024, FBI Oklahoma learned that an individual who goes by the Kik username "itsdirt7863" used the cellular instant messaging application Kik[1] to communicate regarding child pornography and child abuse. "Itsdirt7863" had communicated with a person utilizing the username "freakyfam69" on August 7, 2024. The communications back-and-forth included chats wherein "freakyfam69" stated he has 12 children and has sexual relations with his daughter and son, who are as young as four years old. The communication between "Itsdirt7863" and "freakyfam69" also included sending and receiving child pornography to include a 1 minute and 1 second video of a young female approximately 8 to 10 years old, naked laying on her back with an adult male penis penetrating her vagina, and a 1 minute and 43 second video of a young

[1] Kik is a mobile application-based communication service owned by MediaLab.ai Inc. and headquartered in Santa Monica, California. Kik's Guide for Law Enforcement describes Kik as a "free smartphone messenger application that lets users connect with their friends the world around them through chat." Kik uses WiFi and cellular networks to send and receive messages, images, and videos between Kik users. These communications bypass Short Message Service ("SMS").

female approximately 3 to 5 years of age, naked from waist down laying on a bed with her genitals exposed. At 9 seconds of the video, a naked adult male is seen penetrating the young female's vagina with his penis..

17. During their communications, "Freakyfam69" stated to Kik user "itsdirt7863" that he enjoys children ages 6 to 14 years old and that one of his daughters "…was throwing it back at 3". Based on my training and experience, I believe this to be a reference to having sexual intercourse. "Freakyfam69" and "itsdirt7863" exchanged their locations, wherein "freakyfam69" said he is in Allentown, Pennsylvania and "itsdirt7863" stated he was in Oklahoma City. "Freakyfam69" messaged that he is willing to travel with his children, stating, "If I get plane tickets are kool to hang cause I'll bring any age 2 – 12 is my age cause I always look at them when I'm fucking when they touch my dick a lot more and put it into them".

18. Law enforcement subsequently received information from Kik that the subscriber using the moniker "freakyfam69" utilized an iPhone and the Gmail account goldmusicsoul3@gmail.com to register his Kik account. Additionally, Kik provided law enforcement with various login IP addresses used by "freakyfam69" during August 2024. Specifically, on August 7, 2024, "freakyfam69" used IP addresses that began with a "172…" and also an IP address 216.164.242.105. The "172…" IP addresses belong to T-Mobile, but T-Mobile informed law enforcement that they did not have record of which users utilize those IP addresses.

19. Law enforcement was able to determine that the IP address of 216.164.242.105 is utilized by an Allentown-based internet provider, RCN Telecom. Legal process for the subscriber information for RCN Telecom IP address 216.164.242.105 revealed an address of 1949 Meadows Road, Bethlehem, PA 18015, with a subscriber whose initials are S.J. Again, the

user of "freakyfam69" previously stated that he lives in Allentown, so his use of an Allentown-based IP address corroborated his location.

20. Notably, on August 7, 2024, when "freakyfam69" utilized IP address 216.164.242.105 and IP addresses beginning in "172…," he sent a 1 minute and 1 second video to "itsdirt7863" depicting a nude minor female approximately 8 to 10 years old laying on her back while an adult male penis penetrated her vagina.

21. Law enforcement then served legal process upon Google to obtain information relating to goldmusicsoul3@gmail.com, the associated email account used to register the suspect Kik account, as well as IP login information relating to the email account. Google informed law enforcement that the email goldmusicsoul3@gmail.com was subscribed to by EARL BURFORD, 8435 Williams Avenue, Philadelphia, Pennsylvania 19150, with (407) 376-9881 listed as the recovery phone number.

22. Google also provided information to law enforcement that the Google Pay associated with this Gmail account was for the same subscriber: EARL BURFORD, 8435 Williams Avenue, Philadelphia, Pennsylvania 19150 with (407) 376-9881 listed as the phone number. Google also provided law enforcement with IP addresses that were used to access the Google account between August 24 and August 31, 2024. The IP addresses included IP address 216.164.242.105, which is tied to 1949 Meadows Road, Bethlehem, PA 18015 (see paragraph 19 above), as well as IP addresses which were determined to be registered to T-Mobile, consistent with the information provided by Kik. As set forth below, we have learned that 1949 Meadows Road – and not 8435 Williams Avenue – is BURFORD's address.

23. In September 2024, FBI Philadelphia requested from T-Mobile the subscriber information for the IP addresses provided by Google. T-Mobile provided the subscriber of the IP

addresses as EARL BURFORD, with an active telephone number of (407) 376-9881 and a home address of 1827 Willow Park Road, Bethlehem, Pennsylvania 18020, which is in the Allentown-area, but which we believe is not BURFORD's most recent address. T-Mobile also provided IMEI 354696407172698 as the IMEI number for the cellular telephone assigned call number (407) 376-9881. Law enforcement conducted an open-source check of the IMEI provided by T-Mobile, and it belongs to an Apple iPhone 12. Again, according to Kik, the user of "freakyfam69" used an iPhone to register that account.

24. Legal process served upon T-Mobile for information relating to the subscriber of (407) 376-9881, revealed it is registered to EARL BURFORD, 1827 Willow Park Road, Bethlehem, PA 18020.

25. On September 6, 2024, the Hon. Pamela A. Carlos, United States Magistrate Judge for the Eastern District of Pennsylvania issued an order authorizing the installation and use of a pen register/trap and trace device ("PRTT") to record, decode, and/or capture all dialing, routing, addressing and signaling information associated with each communication to or from the cellular telephone number (407) 376-9881, as well as a warrant authorizing law enforcement to obtain location information for the cellular telephone assigned call number (407) 376-9881.

26. The FBI began receiving data on September 7, 2024. A review of the data showed that the user of the cellular telephone assigned call number (407) 376-9881, was within the area of 1949 Meadows Road, Bethlehem, PA 18015 during late night and early morning hours. Again, 1949 Meadows Road is the physical address associated with IP address 216.164.242.105, which was utilized by "freakfam69."

27. FBI agents conducted surveillance related to 1949 Meadows Road, Bethlehem, PA 18015 on multiple occasions. Agents identified one vehicle matching the description of a

vehicle registered to EARL BURFORD, that is, an Infinity QX 50, which was parked near the detached garage at 1949 Meadows Road, Bethlehem, PA 18015. Based off his Pennsylvania driver's license photo, agents identified an adult male matching the description of EARL BURFORD entering the garage. The agents also identified multiple secured Wi-Fi networks within range of 1949 Meadows Road, Bethlehem, PA 18015. Agents subsequently confirmed with the owners of 1949 Meadows Road that BURFORD resided in their garage.

28. Based on this information, I believe that "freakfyam69" is EARL BURFORD and that he utilized telephone number (407) 376-9881 and email address goldmusicsoul3@gmail.com. .

29. On September 25, 2024, Apple Inc. notified law enforcement that the telephone number (407) 376-9881 is also associated with Apple's FaceTime and iMessage services.

30. On September 30, 2024, Apple Inc. notified law enforcement that EARL BURFORD registered for an Apple account on December 25, 2021, utilizing his email address goldmusicsoul3@gmail.com. On February 25, 2022, BURFORD registered an iPhone 12 utilizing his email address goldmusicsoul3@gmail.com and telephone number (407) 376-9881.

BACKGROUND CONCERNING APPLE[2]

31. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

2 The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security,"

32. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and

---

available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

33. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime)

only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

34. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

35. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My"

service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

36. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

37. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service

("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

38. In child pornography distribution cases, individuals utilizing the devices are not sedentary. In fact, there were multiple IP addresses used for the Kik account to distribute the child pornography. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

39. Additionally, it is common, as noted above, that individuals that distribute child pornography keep those images. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

40. The user of the Kik account that distributed child pornography, did not use his government name but the moniker "freakyfam69." The information contained in the iCloud account would establish attribution. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or

controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

41. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

42. In this investigation, the application used on an iPhone was Kik. It is common for individuals to use more than one application to communicate with others about child pornography or the distribution of child pornography. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can

lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

43. The email account goldmuiscsoul3@gmail.com was used to register to Kik, was used for registering Google Pay, and was used for the Apple account. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CHARACTERISTICS COMMON TO CHILD PORNOGRAPHY COLLECTORS

44. I know from my training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography may collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals may also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography may often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance

and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography may maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often may collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. However, some individuals may dispose of their collections of their sexually explicit materials or only seek out child pornography when they want to view it, in order to conceal their activities for fear of being caught.

g. Where such material is accessed and/or maintained on an Apple iPhone, such materials is often preserved on the user's iCloud account.

h. Based upon my training and experience, I know that some users who

possess, receive, distribute, or produce child pornography transfer these files between their different storage devices and online accounts, whether it is to conceal the files or store them in one account versus another account. I have investigated cases where users transfer child pornography files between devices and/or online accounts, and commonly use email or other online messaging accounts to complete the transfer.

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

s/ Francis Nero
Francis Nero
Special Agent
Federal Bureau of Investigation

Sworn and subscribed
before me this day
of October 2024.

Pamela A. Carlos Digitally signed by Pamela A. Carlos
Date: 2024.10.09 16:48:29 -04'00'

HONORABLE PAMELA A. CARLOS
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with **goldmusicsoul3@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 24, 2024, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of distribution of child pornography, in violation of 18 U.S.C. § 2252(a), those violations involving EARL BURFORD and occurring after August 6, 2023 including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating possessing and distributing child pornography to include stored text messages (SMS and MMS); both read and unread, sent and unsent; contents of the stored address book; telephone call logs; pictures and/or videos stored on the subject device (along with any metadata associated with these files); sent and/or received audio files; evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted; such as logs, phonebooks, saved usernames and passwords, documents, and browsing history; list of installed application and any data associated with, created, or stored by these applications to include location history, chat history and/or shared pictures or videos as they related to offenses described in the affidavit.

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to the distribution of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.